UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

UNITED STATES OF AMERICA, Plaintiff, vs. DAVID BUSBY, Defendant.	Case No: CR 11-00188 SBA **ORDER GRANTING IN PART AND DENYING IN PART DEFENDANT'S MOTION TO SUPPRESS** Dkt. 17

Defendant David Busby is charged in a one-count Indictment with a violation of 18 U.S.C. § 2252(a)(4)(B)—Possession of Child Pornography. The parties are presently before the Court on Defendant's Motion to Suppress Evidence. Dkt. 17. The parties appeared in Court on December 5, 2011, through their counsel of record for oral argument on the motion. Having considered the papers filed in connection with this matter as well as the arguments of counsel at the motion hearing, and being fully informed, the Court hereby GRANTS IN PART and DENIES IN PART the motion for the reasons set forth below.

I. BACKGROUND

A. FACTUAL SUMMARY

1. Seizure of Defendant's Workplace Computers

In or about 2010, Defendant was employed by the Lawrence Berkeley National Laboratory ("LBL") in its Information Technology Division. Smock Decl. Ex. C at DB-11, Dkt. 17. Defendant worked at LBL's Oakland Scientific Facility site located in Oakland, California. Id.

During the morning of April 20, 2010, an off-site cyber security contractor with the National Energy Research Scientific Computing Center ("NERSC")[1] was conducting a routine log analysis of LBL's server. Id., Ex. A at DB-18, 19. The contractor noticed an unusual amount of internet traffic to domain names ending in .biz and .info, preceded by entries such as "tinymodel," "young-angels," "party-models," "newstar-bambi," and "skygirls." Id. In addition, the contractor determined that LBL's server was being used to access bittorrent files with names such as "Taboo-Incest-Father-And-Daughter-Have-Sex-But-Busted-By-Moms-Hidden-Camera-Pthc-Porn-2007-incest" and "Pthc-Russia10Yo-11Yo-Little-Brother-And-Sister-2BoyGirls-Fucking-Just-Posing-Or-Naked-Pthc-R." Id. at DB-19, DB-20. The contractor isolated the entries to a single Internet Protocol ("IP") address as the source of the traffic, Id. Ex. D at DB-4, and traced the IP address to a laptop computer assigned to the Defendant based on his unique LBL network authentication used to login to his computer. Id. Ex. C at DB-10.

Later in the afternoon, LBL's Director of Security contacted the University of California Police Department ("UCPD") to report that an employee was visiting websites that potentially host child pornography. Id. Ex. D at DB-4. LBL's cyber security team went to the Oakland facility and seized Defendant's MacBook Pro laptop computer, which subsequently was turned over to UCPD Detective Nicole Miller. Id. After receiving authorization from LBL's legal counsel, Detective Miller searched the contents of the laptop hard drive which "revealed photographs of an individual possibly in her mid-teens" who was clothed, but was "posed in a provocative manner." Id. The following day on April 21, 2010, UCPD detectives seized eight additional computers used by the Defendant. Id. at DB-5. The search and seizure of Defendant's computers was accomplished without a warrant; however, Defendant had previously signed an acknowledgement that he had "no

[1] NERSC is the primary scientific computing facility for the Office of Science in the United States Department of Energy ("DOE") and is a division of LBL. See Gov. Opp'n at 3 n.1, Dkt. 21.

explicit or implicit expectation of privacy" with respect to LBL computers and servers. Gov. Ex. 1 at DB-61.[2]

2. Application for Search Warrant

On April 21, 2010, UCPD Detective Sabrina Reich applied for a warrant from the Alameda County Superior Court to search Defendant's residence in Richmond, California. Id. Ex. C. The following facts were cited in the probable cause affidavit: (1) LBL had seized Defendant's laptop that was being used to visit "suspected child pornography websites"; (2) LBL had informed UCPD that the laptop was issued to Defendant for use at work and at home; (3) LBL had knowledge that Defendant had previously taken the laptop to his residence; (4) LBL consented to UCPD's warrantless search of the laptop; (5) UCPD made a forensic copy of the computer hard drive and found "several photographic files on [Defendant's] user account…of females in their mid-to-late-teens posing in a sexually suggestive manner and some with buttocks and breasts exposed"; (6) UCPD found "decoding and video viewing files on [Defendant's] laptop" and noted that "sexual offenders are known to use such programs to transfer child pornography . . . [and the] laptop also contained a program that is commonly used to disguise the downloading of large files or large volumes of data on a computer network." Id. at DB-10, DB-11.

Detective Reich further stated that she knew Defendant was a "sex registrant" based on his "prior sex registration appointments and police contacts," and that he had a "prior registerable [sic] offense for 288(a) PC: Lewd & Lascivious Acts w/ Child Under 14, for molesting his 7-to-8 year old step daughter." Id. at DB-11. In examining Defendant's laptop, the Detective discovered numerous "files of interest on [Defendant's] computer user account" including one of: "a female, mid-to-late teens, mixed race, sitting with genital area/underwear exposed." Id. at DB-12. Based on her "training and experience and in

[2] The LBL computer policy states: "Users have no explicit or implicit expectation of privacy. NERSC retains the right to monitor the content of all activities on NERSC systems and networks and access any computer files without prior knowledge or consent of users, senders or recipients. NERSC may retain copies of any network traffic, computer files or messages indefinitely without prior knowledge or consent." Id. Ex. A at DB-61.

conversations . . . with other law enforcement officers," Detective Reich opined that because of the female's general appearance, clothing style, hair style and makeup, "[the] files contain illegal child pornography as specified in Penal Code § 311.1, a felony." Id.

The warrant affidavit also contained "boilerplate" language regarding the characteristics of those who "produce, trade, distribute or possess images or pictures of minors engaged in sexually explicit conduct." Id. One such characteristic is the hoarding of pornographic images of children in electronic devices in "their home, their vehicle, their work areas, and other areas under their control." Id. Combined with witness statements from LBL personnel that claimed "[Defendant] used his unique LBL authentication to access suspected child pornography websites using his work-issued laptop," Detective Reich concluded that additional evidence of child pornography stored in various formats would be discovered at Defendant's residence. Id. Judge Panetta of the Alameda County Superior Court issued the warrant at 4:15 p.m. on April 21, 2010. Id. at DB-7.

3. Interview of Defendant and Execution of Search Warrant

At approximately 2:45 p.m. the following day on April 22, 2010, Detectives Reich and Miller visited Defendant's home to interview him. Id. Ex. J at DB-33; Gov. Ex. 4.[3] The Detectives asked for and were granted permission to enter the home by Defendant and his wife. Id. The Detectives were dressed in plain clothes, although Defendant believed they were armed based on "bulges" in their jackets. Busby Decl. ¶ 8. During the interview, Defendant denied molesting any children since his previous conviction, but admitted to being addicted to pornography. Gov. Ex. 4. At one point, Defendant indicated that he had been through this process before and did not wish to make any statements without legal counsel. Id. Defendant then inquired whether he was under arrest. Id. Detective Reich stated he was not. Id. During the course of the approximately twelve-minute interview, Detective Reich again informed Defendant that he was not under arrest and that they simply

[3] A recording of the interview was reviewed by the Court in connection with the instant motion. The Court notes that the tenor of the interview was calm and akin to a non-confrontational conversation.

wanted to hear what he had to say. Id. Defendant's wife—identified as "Lorna"—was also present during the interview. Id. There is no indication in the record that Defendant was aware that the detectives had a search warrant for his home.

At the end of the interview, Detective Reich asked for Defendant's cooperation in gathering any computers or similar devices from his residence. Id. Defendant indicated he did not have any computers at his home. Id. Detective Reich then informed him that she had a search warrant and was looking for computers, electronic devices, any printed pornographic materials, or videos. Id. At that point, Detectives Reich and Miller were joined by other law enforcement officers who performed the search and uncovered and seized various items including a laptop computer, numerous hard drives, and pornographic DVDs. Id. Ex. J.

4. Federal Agents Interview Defendant at His Residence

Approximately two weeks after Detectives Reich and Miller served the search warrant on the Defendant, DOE Special Agents Quenton Sallows and Nick Williamson interviewed Defendant at his home at around 1:00 p.m. on May 6, 2010. Smock Decl. Ex. K; Gov. Ex. 5 ¶ 2. The Agents identified themselves and asked to speak with Defendant. Gov. Ex. 5 at DB-39. Defendant invited them into his home. Id. At the outset, Agent Sallows informed Defendant he was not under arrest. Id. Subsequently, Defendant admitted to downloading and viewing child pornography on his work computer. Id. Defendant told the Agents they would likely find child porn on the cache files on his computers. Id. Defendant indicated "that he would download the images, place them in an untitled file, and then eventually delete the images from the computers." Id. Despite his admissions, the Agents did not arrest Defendant, and told him that he would be able to self-surrender when it came time for his arrest. Id.

B. PROCEDURAL HISTORY

On March 31, 2011, Defendant was indicted on one count of possession of child pornography in violation of 18 U.S.C. § 2252(a)(4)(B). Dkt. 1. Defendant was arrested on April 1, 2011. Dkt. 9. He posted bond on April 13, 2011 and was released. Bond, Dkt. 11.

On July 5, 2011, Defendant filed the instant motion to suppress alleging violations of his Fourth and Fifth Amendment rights. Defendant contends that the warrantless search of his laptop and other LBL computers was illegal and seeks to suppress evidence seized from them. He also seeks to suppress the evidence seized from his home on the ground that the search warrant application failed to disclose sufficient probable cause. In that regard, Defendant seeks a Franks hearing to address alleged material misrepresentations by the affiant, Detective Reich. In the alternative, Defendant seeks to suppress the statements he made to the UCPD detectives and DOE agents on the grounds that he was not Mirandized. The motion has been fully briefed and is ripe for adjudication.

II. LEGAL STANDARD

The Fourth Amendment protects individuals against unreasonable searches and seizures. U.S. Const. amend. IV. Any evidence resulting from an unconstitutional search or seizure cannot be admitted as proof against the victim of the search, and therefore must be suppressed. See Wong Sun v. United States, 371 U.S. 471, 485 (1963). The Supreme Court has held that "the proponent of a motion to suppress has the burden of establishing that his own Fourth Amendment rights were violated by the challenged search or seizure." United States v. Caymen, 404 F.3d 1196, 1199 (9th Cir. 2005) (citing Rakas v. United States, 439 U.S. 128 (1978)). The strictures of the Fourth Amendment also apply to the conduct of government officials. O'Connor v. Ortega, 480 U.S. 709, 715 (1987) ("[s]earches and seizures by government employers… are subject to the restraints of the Fourth Amendment.").

III. DISCUSSION

A. SEIZURE OF DEFENDANT'S LAPTOP AND COMPUTERS

A criminal defendant "may invoke the protections of the Fourth Amendment only if he can show that he had a *legitimate* expectation of privacy in the place searched or the item seized." United States v. Zeigler, 474 F.3d 1184, 1189 (9th Cir. 2007) (citing Smith v. Maryland, 442 U.S. 735, 740 (1979)). The "legitimate expectation of privacy" inquiry has both a subjective and an objective component. Smith v. Maryland, 442 U.S. 735, 740-

41 (1979) (citing Katz v. United States, 389 U.S. 347 (1967)). The subjective element looks to whether the individual "exhibited an actual (subjective) expectation of privacy," while the objective element assesses whether the subjective expectation of privacy is "one that society is prepared to recognize as 'reasonable.'" Id. at 740-41.

As a general matter, courts have found that an employee's expectation of privacy in files stored on a work-issued computer is not objectively reasonable where the employer notifies employees that their computer files are subject to monitoring. See United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000) (holding that government employee's belief that his computer files were private was not objectively reasonable where the employer's policy reserved its right to "audit, inspect, and monitor" his computer files); United States v. Angevine, 281 F.3d 1130, 1134 (10th Cir. 2002) (upholding denial of defendant professor's motion to suppress child pornography located on the erased files on his office computer which was part of a university network where the university's computer use policy notified users that internet activity was subject to monitoring); Sporer v. UAL Corp., No. C 08-02835 JSW, 2009 WL 2761329, at *5 (N.D. Cal. Aug. 27, 2009) (finding that employee lacked a reasonable expectation of privacy in his work email where the employer had a policy of monitoring its employee's computer use and warned employees that they had no expectation of privacy on e-mail transmitted on the company system); Wasson v. Sonoma County Junior Coll., 4 F. Supp. 2d 893, 905-906 (N.D. Cal. 1997) (employer's computer policy giving it "the right to access all information stored on [the employer's] computers" defeated employee's reasonable expectation of privacy in files stored on employer's computers); but see United States v. Heckenkamp, 482 F.3d 1142, 1147 (9th Cir. 2007) (university student had a reasonable expectation of privacy in files on his personal computer connected to the university network where the university had "no announced monitoring policy on the network").

Here, there is no dispute between the parties that during the relevant time period, LBL maintained a computer use policy which made it clear to users that they have no

expectation of privacy on any LBL computers or its network. The policy states, in relevant part, that:

> **Monitoring and Privacy**
>
> *Users have no explicit or implicit expectation of privacy.* NERSC retains the right to monitor the content of all activities on NERSC systems and networks and access any computer files without prior knowledge or consent of users, senders or recipients. NERSC may retain copies of any network traffic, computer files or messages indefinitely without prior knowledge or consent.

Gov. Ex. 1 at DB-61 (emphasis added). On December 9, 2009, Defendant signed an acknowledgement of the foregoing policy. Id. at DB-61 ("I have read the NERSC Policies and Procedures and understand my responsibilities in the use of NERSC resources.").[4] LBL's computer use policy was reinforced through the use of network security banners displayed on its computers, which notified users that their activities were subject to monitoring and interception. Id. Ex. 2 ¶ 3(a)-(b). Moreover, Defendant was well aware that LBL employees have no expectation of privacy with respect to their use of LBL computers, given Defendant's employment in the Information Technology Division at LBL and his responsibility for maintaining the network security banners for certain user groups at LBL. Id. ¶ 4. Thus, given the weight of authority cited above, the Court finds that Defendant lacked an *objectively* reasonable expectation of privacy in his assigned laptop and its contents.

Notably, Defendant does not dispute that he was aware of and bound by LBL's computer use policy. Rather, he argues for the first time in his reply that he had a reasonable expectation of privacy because: LBL issued the laptop to him specifically; he was responsible for installing and maintaining software on the laptop; access to the laptop required a log-in and password; and that, as a practical matter, he used the laptop for both work and personal activities. Def.'s Reply at 3; Busby Reply Decl. ¶¶ 2-5. Defendant's

[4] In addition, all LBL employees are required (and were required in April 2010) to take a cyber security refresher course which requires users to acknowledge their understanding that their use of LBL computers and network is subject to monitoring, and that they have no expectation of privacy in their use thereof. Welcher Decl. ¶ 2, Dkt. 21-2.

arguments, however, are germane to his *subjective* expectation of privacy—*not* to whether his expectation was *objectively* reasonable. In addition, Defendant fails to confront the fact that the laptop was the LBL's property and, at all relevant times, was subject to LBL's monitoring policy. As noted, that policy unequivocally provides that "[u]sers have no explicit or implicit expectation of privacy" and that LBL has unfettered discretion to "access any computer files without prior knowledge or consent of users[.]" Gov. Ex. 1 at DB-61.

As an ancillary matter, Defendant argues that LBL's computer use policy only permits LBL to monitor its employees' computers for "computer security purposes," but not to conduct criminal investigations. Def.'s Reply at 4-5. As support for this alleged distinction, Defendant points out that section 9.02 of LBL's Rules and Procedures Manual ("RPM") contains no specific procedure for seizing and searching an employee's computer.[5] It is unclear, however, how the absence of specific procedures for the search and seizure of a LBL computer necessarily compels the conclusion that Defendant had an objectively reasonable expectation of privacy in this instance. Indeed, the RPM reiterates that LBL employees have no such expectation. Section 9.01(D) of the RPM states, in pertinent part:

> **D. CONSENT TO MONITORING**
>
> All use of LBNL computing and communications resources by all users, including employees, guests, collaborators, and casual users, is subject to monitoring. *No user of LBNL systems has any expectation of privacy in their use of these systems, subject to applicable State, Federal, Department of Energy, and University law and policy.*

RPM § 9.01(D) (emphasis added). In addition, the RPM clearly states that personal or "incidental" use of LBL computer is permissible, but that "[u]sers who elect to engage in incidental use do so with *no expectation of personal privacy* concerning their actions." Id. § 9.01(F)(2) (emphasis added). Thus, if anything, the RPM undermines any claim by

[5] Section 9 of the RPM is available at: http://www.lbl.gov/LBL-Work/RPM/ (last visited Nov. 28, 2011).

Defendant that he had a legitimate expectation of privacy in his use of LBL-issued computers.

In sum, the Court finds that Defendant lacked a legitimate expectation of privacy with respect to files stored on the laptop and other LBL computers. Therefore, the Court denies Defendant's motion to suppress with respect to such evidence. See United States v. Garcia-Rodriguez, 558 F.2d 956, 960 (9th Cir. 1977) (affirming denial of motion to suppress contraband seized from a warehouse in which defendants lacked a reasonable expectation of privacy).

B. SEARCH OF DEFENDANT'S HOME

Defendant next contends that the search of his home violated his Fourth Amendment rights on the grounds that: (1) the search warrant was based on the allegedly invalid search of his laptop; and (2) the Statement of Probable Cause accompanying the application for the search warrant failed to establish probable cause that a crime had been committed or that contraband likely would be found at his home. Additionally, Defendant requests that the Court hold a Franks hearing to address the alleged misrepresentations of fact in the search warrant application. The Court has concluded above that the search of the laptop was proper. Therefore, the motion is denied on that basis. The Court now turns to the remaining issue of whether there was sufficient probable cause to support the issuance of the search warrant.

1. Legal Standard

"A search warrant, to be valid, must be supported by an affidavit establishing probable cause." United States v. Stanert, 762 F.2d 775, 778 (9th Cir. 1985). Probable cause exists if "there is a fair probability that contraband or evidence of a crime will be found" in the place to be searched. Illinois v. Gates, 462 U.S. 213, 238 (1983); Chism v. Washington State, 655 F.3d 1106, 1114 (9th Cir. 2011). The assessment of probable cause is a "practical, common-sense decision" made in light of the totality of the circumstances. Gates, 462 U.S. at 238. The district court is "limited to the information and circumstances contained within the four corners of the underlying affidavit." Stanert, 762 F.2d at 778.

Review of another judge's probable cause determination is deferential, meaning that "the duty of a reviewing court is simply to ensure that the magistrate had a 'substantial basis for ... conclud[ing]' that probable cause existed." Gates, 462 U.S. at 238-39; accord United States v. Krupa, 658 F.3d 1174, 1180 (9th Cir. 2011).

2. Analysis

The search warrant application submitted by Detective Reich alleged that there was probable cause to believe that evidence of child pornography, in violation of California Penal Code § 311.11, would be found at Defendant's home. Smock Decl. Ex. C at DB-13. Section 311.11 "makes it a public offense for any person, among other things, to possess or control any visual matter, 'the production of which involve[d] the use of a person under the age of 18 years, knowing that the matter depicts a person under the age of 18 years personally engaging in or simulating sexual conduct.'" In re Alva, 33 Cal.4th 254, 262 (2004) (quoting Cal. Penal Code § 311.11(a)). According to the California Supreme Court, "the prohibited matter must depict actual persons, who are actually under 18, engaged in actual or simulated sex acts, and the violator must know that this is so." Id.

The Government contends that probable cause for the issuance of the search warrant was established by: (1) information from an LBL cyber security employee that a laptop traced to the Defendant was being used to access unspecified "suspected child pornography websites"; (2) the affiant's description of the nine "files of interest" found on the laptop hard drive which allegedly "contain illegal child pornography as specified in Penal Code § 311.1, a felony"; (3) the affiant's awareness that the Defendant took his laptop home on occasion and her opinion that collectors of child pornography tend to make copies of downloaded files of pornographic images which they store at home and work; and (4) evidence that Defendant is a convicted child molester. Gov. Opp'n at 8; Smock Decl. Ex. C at DB-11-12. The Court disagrees that the foregoing information supplied the state court judge with a substantial basis upon which to find probable cause.

First, no facts are alleged in support of the affiant's conclusory assertion that Defendant was using his computer to access child pornographic websites or even

"suspected child pornography websites." Smock Decl. Ex. C at DB-10. The Supreme Court has counseled that "[a]n affidavit must provide the magistrate with a substantial basis for determining the existence of probable cause" and that a "wholly conclusory statement" is insufficient. See Gates, 462 U.S. at 239. In Gates, for example, the Court held that a statement that "[the] 'affiants have received reliable information from a credible person and believe' that heroin is stored in a home" was too conclusory to establish probable cause. Id.; United States v. Dubrofsky, 581 F.2d 208, 212 (9th Cir. 1978) ("A search warrant may not rest upon mere affirmance or belief without disclosure of supporting facts or circumstances."). Here, the affiant failed to provide any specific information concerning the websites, including why the unidentified websites were suspected of hosting child pornography. In the absence of such facts, the affiant's vague assertion that the Defendant used his laptop to "access suspected child pornography websites" is precisely the type of "barebones" assertion which courts have found insufficient to support a finding of probable cause. See Gates, 462 U.S. at 239; c.f. United States v. Gourde, 440 F.3d 1065, 1070 (9th Cir. 2006) (holding that probable cause was established where the search warrant affidavit presented facts showing that the "lolitagirls.com" website accessed by defendant, in fact, contained child pornography) (en banc).[6] No such showing was made in this case.

Second, the affiant's description of the nine "files of interest" found on the laptop hard drive do not support the affiant's showing of probable cause; if anything, they detract from it. The affiant described the models in each of the nine files as a "female, mid to late teens." Smock Decl. Ex. C at DB-11-12. At oral argument, however, the Government conceded that a female in her "late teens" necessarily includes individuals who are 18 and 19 years-old, i.e., adults for purposes of the criminal provisions implicated in this case. Images of a "late teen" would not constitute child pornography under either state or federal law, since both statutes apply only to persons who are *under* the age of 18. Cal. Pen. Code

[6] Detective Reich chose not disclose the names of the websites accessed by the Defendant or the names of Defendant's bittorrent inquiries. By failing to do so, Detective Reich foreclosed the state court judge from engaging any further inquiry to determine whether there was sufficient probable cause to issue the warrant.

§ 311.11; 18 U.S.C. §§ 2252(b)(2), 2256(1).[7] Indeed, the affiant's descriptions are particularly problematic because she chose not to provide the actual images to the state court judge to review. As such, there is nothing in the record to substantiate that the state court judge concluded that the images were that of a minor, as opposed to an adult.

Moreover, the descriptions provided by the affiant do not support her assertion that the files "contain illegal child pornography as specified in Penal Code § 311.1[.]" Smock Decl. Ex. C at DB-12. Section 311.1 makes it illegal to distribute any matter depicting "a person under the age of 18 years personally engaging in or personally simulating sexual conduct, as defined in Section 311.4, . . ." Cal. Pen. Code § 311.1(a). Section 311.4 states, in relevant part:

> "sexual conduct" means any of the following, whether actual or simulated: sexual intercourse, oral copulation, anal intercourse, anal oral copulation, masturbation, bestiality, sexual sadism, sexual masochism, penetration of the vagina or rectum by any object in a lewd or lascivious manner, *exhibition of the genitals or pubic or rectal area for the purpose of sexual stimulation of the viewer*, any lewd or lascivious sexual act as defined in Section 288, or excretory functions performed in a lewd or lascivious manner, whether or not any of the above conduct is performed alone or between members of the same or opposite sex or between humans and animals. An act is simulated when it gives the appearance of being sexual conduct.

Id. § 311.4(d)(1) (emphasis added).[8] Of the nine images discussed by the affiant, only the first image ("8b2905ad8288d6da38720a2e33760d9a—3—greenjpg—large") potentially describes "sexual conduct." With respect to that image, the affiant stated: "This image depicts a female, mid-to-late teens, mixed race sitting with genital area/underwear exposed." Smock Decl. Ex. C at DB-11. But the mere fact that the model was "sitting with genital area/underwear exposed," *without more*, does not convey or suggest that she was

[7] Logically, a female in her "teens" includes a person from the age of 13 to 19. An early teen would be 13 or 14 years-old; a mid teen from 15 to 17 years-old; and a late teen from 18 to 19 years-old. Thus, stated another way, the affiant's reference to "late teens" necessarily includes legal adults.

[8] A "lewd or lascivious act" under Penal Code § 288 is one which involves a child under the age of 14. Cal. Pen. Code § 288(a).

doing so "for the purpose of sexual stimulation of the viewer," as specified in section 311.4(d)(1). See United States v. Battershell, 457 F.3d 1048, 1051 (9th Cir. 2006) (affiant's description of a "young female (8-10 YOA) naked in bathtub," absent an accompanying photograph, was "insufficient to establish probable cause that the photograph lasciviously exhibited the genitals or pubic area because his conclusory statement is an inherently subjective analysis"). Given the affiant's vague description of the photograph, coupled with her failure to provide a copy of the photograph at issue, the state court judge lacked a substantial basis upon which to conclude that "illegal child pornography" had been found on the Defendant's computer.

Third, the fact that Defendant took his laptop home is of little moment given that the LBL had already confiscated his laptop and turned it over to UCPD. As for the affiant's assertion that collectors of child pornography tend to make copies of illicit images and store them at work and home, such information is inapposite because the affiant failed to disclose sufficient information for the state court judge to conclude that the Defendant had, in fact, accessed a child pornography website and/or stored images of child pornography on his computer in the first instance. As such, the state court judge had no legally recognizable factual basis upon which to reach the conclusion that the Defendant likely made copies of child pornography, which then could be found at his home.

The Government contends that even if the descriptions of nine downloaded images were insufficient to establish probable cause, the state court judge could consider that images from the suspected child pornography websites were automatically downloaded to the Defendant's computer as cache files.[9] Gov. Surrreply at 6. However, the affiant did not include this information in her application for a search warrant nor did she represent that the laptop's cache files were searched or that any files from the unidentified websites were

[9] The cache files or temporary files are created when a user visits a website. See United States v. Romm, 455 F.3d 990, 993 n.1 (9th Cir. 2006) ("Most web browsers keep copies of all the web pages that you view, up to a certain limit, so that the same images can be redisplayed quickly when you go back to them.") (internal quotations and citation omitted).

found. As such, the Government's speculative contentions regarding the cache files potentially stored on Defendant's laptop are unavailling. See Crowe v. County of San Diego, 608 F.3d 406, 434 (9th Cir. 2010) ("In reviewing a search warrant on probable cause grounds, … the district court … is limited to the information and circumstances contained within the four corners of the underlying affidavit.") (citation and quotation marks omitted).

Finally, the affiant's disclosure that the Defendant was a convicted child molester, under the particular set of circumstances presented here, does not establish probable cause to search the Defendant's home. See Dougherty v. City of Covina, 654 F.3d 892, 899 (9th Cir. 2011) (holding that affiant's conclusory allegation that the defendant molested two children did not establish probable cause to search for child pornography on his home computer); see also Millender v. County of Los Angeles, 620 F.3d 1016, 1028-29 (9th Cir. 2010) (holding that the defendant's prior felony convictions, membership in a gang and information that he was suspected in an assault with a deadly weapon case did not provide probable cause to search for firearms at defendant's home). In this case, Defendant's child molestation conviction was certainly relevant, under the totality of circumstances, to ascertaining whether probable cause existed to search his home. See Dougherty, 654 F.3d at 899. However, the paucity of information presented by the affiant renders the affidavit insufficient to support a probable cause finding to search Defendant's home for evidence of child pornography. The affiant's disclosure of Defendant's conviction for child molestation under these facts does not assist the Government.

In sum, the Court concludes that the state court judge lacked a substantial basis for finding probable cause to issue a search warrant for Defendant's home. Accordingly, Defendant's motion to suppress is granted and all evidence seized from Defendant's home pursuant to the search warrant issued by the Alameda County Superior Court on April 21, 2010 is suppressed. See Wong Sun v. United States, 371 U.S. 471, 487–88 (1963).

C. SUPPRESSION OF DEFENDANT'S STATEMENTS

Defendant next contends that his statements to the UCPD officers and DOE agents must be excluded based on the agent's failure to Mirandize him. Def.'s Mot. at 15. When a person in custody is subjected to interrogation, he must first be read his Miranda rights in order for the information obtained to be admissible in court. See Miranda v. Arizona, 384 U.S. 436, 467-68 (1966). Miranda rights include the right to remain silent, the right to a retained or appointed attorney, and a warning that anything said may be used in court against the suspect. Id. "Statements elicited in noncompliance with this rule may not be admitted for certain purposes in a criminal trial." Stansbury v. California, 511 U.S. 318, 322 (1994) (per curiam). For purposes of Miranda, custodial interrogation means "questioning initiated by law enforcement officers after a person has been taken into custody or otherwise deprived of his freedom of action in any significant way." Miranda, 384 U.S. at 444. An individual is "in custody" if, based on the totality of the circumstances, "a reasonable person in [the defendant's] position ... would not have felt free to terminate the interrogation" and leave. Craighead, 539 F.3d at 1082. This determination is an objective one. United States v. Bassignani, 575 F.3d 879, 883 (9th Cir. 2009).

The Ninth Circuit has counseled that a number of factors should be considered in determining whether a defendant was in custody during questioning. Relevant to this inquiry are: "(1) the language used to summon the individual; (2) the extent to which the defendant is confronted with evidence of guilt; (3) the physical surroundings of the interrogation; (4) the duration of the detention; and (5) the degree of pressure applied to detain the individual." United States v. Kim, 292 F.3d 969, 973 (9th Cir. 2002) (internal quotation marks omitted). Where, as here, the interrogation occurs in the person's home, the court also may take into account: (1) the number of law enforcement personnel and whether they were armed; (2) whether the suspect was at any point restrained, either by physical force or by threats; (3) whether the suspect was isolated from others; and (4) whether the suspect was informed that he was free to leave or terminate the interview, and

the context in which any such statements were made. United States v. Craighead, 539 F.3d 1073, 1084 (9th Cir. 2008).

Taking into account the above factors, under the totality of the circumstances, the Court finds that Defendant was not in custody when has was interviewed by the UCPD detectives on April 22, 2010. The record shows that only two plain clothed UCPD detectives, Reich and Miller, were present during the interrogation. The audio recording provided by the Government demonstrates that the conversation during this interview was cordial. Gov. Ex. 4. In fact, the officers asked few questions of the Defendant and emphasized that they were merely there to hear what he had to say. Id. Though Defendant states that he could see the officers' guns in their holsters, Busby Reply Decl. ¶ 8, there is no evidence or suggestion that the officers brandished their weapons or otherwise displayed them to Defendant during the course of the twelve-minute interview. There also is no evidence that the Defendant was restrained by force or by threats or handcuffed at any time during the meeting. In addition, Defendant was not alone, as his wife was present during the questioning.

Although the Defendant was not expressly told he could leave, it is significant that the questioning took place at Defendant's home. As the Ninth Circuit observed in Craighead, when the interrogation takes place in a defendant's home, "he is already in the most constitutionally protected place on earth"; thus, this prong is not meaningful in the context of an interrogation conducted in one's home. 539 F.3d at 1083. Despite Defendant's claims to the contrary, the record does not support Defendant's assertion that "his home had become a police-dominated atmosphere" in which he was not "free to ask the officers to leave or to not respond to their questions." Def.'s Reply at 15. Whereas the "presence of a large number of visibly armed law enforcement goes a long way towards making the suspect's home a police-dominated atmosphere," here, a reasonable person would not have concluded that two plain clothed, albeit armed, officers who engaged in cordial conversation with the Defendant created a police-dominated atmosphere. See Craighead, 539 F.3d at 1085.

Defendant's arguments regarding the May 6, 2010 meeting with DOE agents Sallow and Williamson fare no better. See Def.'s Reply at 15. Like the UCPD interview, Defendant met with two agents in his home. Busby Reply Decl. ¶ 13. The agents were dressed in business suits, as opposed to uniforms. Id. Though Defendant has opined that the agents were armed based on the visible "bulges" in their suit jackets, there is no evidence or allegation that they brandished their weapons or used any force or threats of force against him. Nor is there any indication that the Defendant was isolated from anyone or otherwise informed that he was not free to leave or to terminate the interview. To the contrary, Agent Sallow informed Defendant that he was not under arrest, and that when the time came for his arrest, Defendant would be allowed to self-surrender. See Bassignani, 575 F.3d at 886 (defendant is not in custody when he is told he is not under arrest). There is nothing in the record presented to suggest that a reasonable person in Defendant's situation would not have felt free to end the conversation.[10]

[10] Defendant's motion to suppress statements made to these law enforcement officials rests entirely on his Miranda argument. He does not argue or present any evidence showing that there is any nexus between the interviews conducted by the UCPD detectives or the DOE agents and the deficient search warrant. Nor is there any evidence in the record presented suggesting that the "fruits" of the unlawful search on April 22, 2010 induced his statements during the interviews. See United States v. Davis, 332 F.3d 1163, 1171 (9th Cir. 2003). As such, the Court declines to sua sponte consider the issue of whether the validity of the search warrant has any bearing on the suppression of the statements. However, the denial of Defendant's motion to suppress his statements is without prejudice, and Defendant may renew this aspect of his motion provided that there is a factual and legal foundation for doing so.

IV. CONCLUSION

For the reasons set forth above,

IT IS HEREBY ORDERED THAT Defendant's Motion to Suppress Evidence is GRANTED with respect to evidence seized from Defendant's home pursuant to the search warrant issued by the Alameda County Superior Court on April 21, 2010, and DENIED in all other respects.

IT IS SO ORDERED.

Dated: December 14, 2011

SAUNDRA BROWN ARMSTRONG
United States District Judge